

(19)日本国特許庁(JP)

(12) 公開特許公報 (A)

(11)特許出願公開番号

特開2003-67210

(P2003-67210A)

(43)公開日 平成15年3月7日(2003.3.7)

(51)Int.Cl.

識別記号

FI

テロート(参考)

G06F 11/00

G06F 9/06

660N 5B076

審査請求 未請求 請求項の数8 OL (全13頁)

(21)出願番号 特願2001-251925(P2001-251925)

(22)出願日 平成13年8月22日(2001.8.22)

(71)出願人 390024350

株式会社ジャストシステム

徳島県徳島市沖浜東3-46

(72)発明者 豊田 光樹

徳島市沖浜東3丁目46番地 株式会社ジャ
ストシステム内

(74)代理人 100104190

弁理士 酒井 昭徳

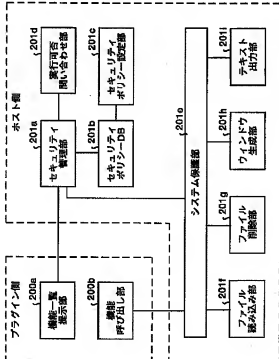
Fターム(参考) 58076 FD08

(54)【発明の名称】 プログラム実行防止装置、プログラム実行防止方法、その方法をコンピュータに実行させるプログラムおよびそのプログラムを記録したコンピュータ読み取り可能な記録媒体

(57)【要約】

【課題】 ウィルスに感染したプログラムや何らかの悪意をもって作成されたプログラムなど、ユーザやシステムにとって危険なプログラムの実行を未然に防止すること。

【解決手段】 プラグインのインストールあるいは起動に先立って、その機能一覧提示部200aはホストとなるアプリケーションに対し、当該ホストから呼び出して使用する機能(サービス)の一覧を提示する。ホストのセキュリティ管理部201aは、上記一覧中にあらかじめ指定された危険な機能(ファイル削除など)が含まれる場合に、実行可否問い合わせ部201dによりそれぞれインストール/起動をおこなうかどうかをユーザに問い合わせる。またプラグインの実行中には、実際に呼び出された機能が上記で提示されたものでなかった場合に、当該プラグインの実行を継続するかどうかを随時間問い合わせる。



【特許請求の範囲】

【請求項1】 その実行にユーザの許可が必要な機能を指定する指定手段と、

プログラムから提示された機能一覧中に前記指定手段により指定された機能が含まれるか否かを判定する判定手段と、

前記判定手段により前記機能一覧中に前記指定された機能が含まれると判定された場合に、前記プログラムをインストールするか否かをユーザに問い合わせる問い合わせ手段と、

を備えたことを特徴とするプログラム実行防止装置。

【請求項2】 その実行にユーザの許可が必要な機能を指定する指定手段と、

プログラムから提示された機能一覧中に前記指定手段により指定された機能が含まれるか否かを判定する判定手段と、

前記判定手段により前記機能一覧中に前記指定された機能が含まれると判定された場合に、前記プログラムを起動するか否かをユーザに問い合わせる問い合わせ手段と、

を備えたことを特徴とするプログラム実行防止装置。

【請求項3】 その実行にユーザの許可が必要な機能を指定する指定手段と、

プログラムから呼び出された機能が前記指定手段により指定された機能であるか否かを判定する第1の判定手段と、

前記第1の判定手段により前記呼び出された機能が前記指定された機能であると判定された場合に、前記呼び出された機能が前記プログラムから提示された機能一覧中に含まれていたか否かを判定する第2の判定手段と、前記第2の判定手段により前記呼び出された機能が前記プログラムから提示された機能一覧中に含まれていなかったと判定された場合に、前記プログラムの実行を継続するか否かをユーザに問い合わせる問い合わせ手段と、を備えたことを特徴とするプログラム実行防止装置。

【請求項4】 その実行にユーザの許可が必要な機能を指定する指定手段と、

プログラムから提示された機能一覧中に前記指定工程で指定された機能が含まれるか否かを判定する判定工程と、

前記判定工程で前記機能一覧中に前記指定された機能が含まれると判定された場合に、前記プログラムをインストールするか否かをユーザに問い合わせる問い合わせ工程と、

を含んだことを特徴とするプログラム実行防止方法。

【請求項5】 その実行にユーザの許可が必要な機能を指定する指定工程と、

プログラムから提示された機能一覧中に前記指定工程で指定された機能が含まれるか否かを判定する判定工程と、

前記判定工程で前記機能一覧中に前記指定された機能が含まれると判定された場合に、前記プログラムを起動するか否かをユーザに問い合わせる問い合わせ工程と、を含んだことを特徴とするプログラム実行防止方法。

【請求項6】 その実行にユーザの許可が必要な機能を指定する指定工程と、

プログラムから呼び出された機能が前記指定工程で指定された機能であるか否かを判定する第1の判定工程と、前記第1の判定工程で前記呼び出された機能が前記指定された機能であると判定された場合に、前記呼び出された機能が前記プログラムから提示された機能一覧中に含まれていたか否かを判定する第2の判定工程と、

前記第2の判定工程で前記呼び出された機能が前記プログラムから提示された機能一覧中に含まれていなかったと判定された場合に、前記プログラムの実行を継続するか否かをユーザに問い合わせる問い合わせ工程と、を含んだことを特徴とするプログラム実行防止方法。

【請求項7】 前記請求項4～請求項6のいずれか一つに記載の方法をコンピュータに実行させるプログラム。

【請求項8】 前記請求項7に記載のプログラムを記録したコンピュータ読み取り可能な記録媒体。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】この発明は、ユーザあるいはシステムにとって危険なプログラムの実行を未然に防止するプログラム実行防止装置、プログラム実行防止方法、その方法をコンピュータに実行させるプログラムおよびそのプログラムを記録したコンピュータ読み取り可能な記録媒体に関する。

【0002】

【従来の技術】企業や大学などの大規模な組織体では、早くからその構内のコンピュータを相互に接続するネットワーク（LAN）の整備が進んでいたが、近年はPCベースのクライアント/サーバシステムが容易に、かつ安価に導入できることもあり、中小企業や個人家庭などにおいてもその保有する複数のコンピュータのネットワーク化が急速に進んでいる。

【0003】また、ここ数年のインターネットの爆発的な拡大により、コンピュータはスタンドアロンで使用されるより、インターネットに接続されて使用されることのほうがむしろ一般的となってきた。さらに、最近は常時接続もめずらしくなくなり、インターネットに接続されたコンピュータの個数だけでなく、個々のコンピュータの接続時間もますます増大する傾向にある。

【0004】ただ、ネットワーク内の他のコンピュータとのデータ交換は、その利便性的一方で、当該ネットワークに侵入したコンピュータ・ウィルスに対して絶好の増殖の機会を提供していることにもなる。昨年5月に世界中で蔓延した「I love you」ウィルス（正確にはワーム）は、インターネットのメールアドレスを

通じてまたたく間に拡がり、それにより発生した有形・無形の被害の総額ははかりしれない。

【0005】

【発明が解決しようとする課題】そして、このようなウイルスによる損害の発生を未然に回避するため、ウイルス検出・駆除のためのソフトウェアも市販されているが、これによる検出・駆除はその原理上どうしても「後追い」となり、未知のウイルスには対応できないこと、次々と開発され巧妙化する新種のウイルスとの「いたちごっこ」になってしまうこと、などの問題点があった。

【0006】すなわちこれらのソフトウェアでは、ブートセクタ、システムメモリ、パーティションテーブル、ファイルなど、ウイルス感染の可能性のあるあらゆる場所について、特定のウイルスに固有なコード群（パターン）の有無をチェックし、発見したコード群からウイルスを特定する。

【0007】このような原理であるため、ウイルスとその固有のコード群とを対応づけた一覧表にないウイルス、たとえばこれまで一度も発見・分析されたことのない未知のウイルスはもちろん、既知のウイルスであってもユーザが一覧表の更新を怠っている場合には、検出・駆除することができない。

【0008】また、Mutation Engine（ウイルスの作成者が単純なウイルスを容易に多形態型に変えられるソフトウェア）のリリース以来、40億もの形態のどれにでもなれる多形態型のウイルスが増加しているが、このタイプのウイルスに含まれるコード群は本来のものから変容されているため、上記手法による検出・駆除が困難になる。

【0009】さらに上記ソフトウェアはもっぱらウイルスの検出・駆除を目的とするものであって、ユーザやシステムにダメージを与えるという点ではウイルスと大差のない、何らかの悪意のあるプログラムを、そうでないプログラムと区別することはできないという本質的な問題を持っている。たとえば、ダイアルアップ先を勝手に変更してしまうActiveXコントロールと、ダイアルアップ先の設定・変更を自動化するために用意されたプログラムとは、いずれもウイルスに感染していない限りは同様に実行が許可されてしまう。

【0010】この点環境によっては、その環境ごとのセキュリティポリシーにもとづいて、ローカルリソースへのアクセスを制限しているものがある。たとえばJavaのVM上で実行されるJavaアプレット（アプリなど）は、その動作するコンピュータ上のファイル（たとえば電話帳など）に一切アクセスすることができない。

【0011】これは安全性という観点からは、非常に強力な確実な防衛方法であるが、その反面で実用的アプリケーションの開発における大きな障害・制限となり、開発者やユーザの利便性が損なわれるという問題がある。

【0012】この発明は、ユーザやシステムにとって危険なプログラム、あるいは少なくともその問題部分の実行を未然に防止することが可能なプログラム実行防止装置、プログラム実行防止方法、その方法をコンピュータに実行させるプログラムおよびそのプログラムを記録したコンピュータ読み取り可能な記録媒体を提供することを目的とする。

【0013】

【課題を解決するための手段】上述した課題を解決し、目的を達成するため、請求項1に記載の発明にかかるプログラム実行防止装置は、その実行にユーザの許可が必要な機能を指定する指定手段と、プログラムから提示された機能一覧中に前記指定手段により指定された機能が含まれるか否かを判定する判定手段と、前記判定手段により前記機能一覧中に前記指定された機能が含まれると判定された場合に、前記プログラムをインストールするか否かをユーザに問い合わせる問い合わせ手段と、を備えたことを特徴とする。

【0014】この請求項1に記載の発明によれば、あらかじめ指定された処理をおこなうプログラムについては、インストールに先立ってユーザにその事実が警告されるとともに、ユーザが指示した場合には当該インストールが中止される。

【0015】また、請求項2に記載のプログラム実行防止装置は、その実行にユーザの許可が必要な機能を指定する指定手段と、プログラムから提示された機能一覧中に前記指定手段により指定された機能が含まれるか否かを判定する判定手段と、前記判定手段により前記機能一覧中に前記指定された機能が含まれると判定された場合に、前記プログラムを起動するか否かをユーザに問い合わせる問い合わせ手段と、を備えたことを特徴とする。

【0016】この請求項2に記載の発明によれば、あらかじめ指定された処理をおこなうプログラムについては、起動に先立ってユーザにその事実が警告されるとともに、ユーザが指示した場合には当該起動が中止される。

【0017】また、請求項3に記載のプログラム実行防止装置は、その実行にユーザの許可が必要な機能を指定する指定手段と、プログラムから呼び出された機能が前記指定手段により指定された機能であるか否かを判定する第1の判定手段と、前記第1の判定手段より前記呼び出された機能が前記指定された機能であるとして判定された場合に、前記呼び出された機能が前記プログラムから提示された機能一覧中に含まれていたか否かを判定する第2の判定手段と、前記第2の判定手段により前記呼び出された機能が前記プログラムから提示された機能一覧中に含まれていなかったと判定された場合に、前記プログラムの実行を継続するか否かをユーザに問い合わせる問い合わせ手段と、を備えたことを特徴とする。

【0018】この請求項3に記載の発明によれば、プロ

プログラムの実行中あらかじめ提示されたとは異なる機能が呼び出されたときは、ユーザにその事実が警告されるとともに、ユーザが指示した場合には当該プログラムの実行が中断される。

【0019】また、請求項4に記載のプログラム実行防止方法は、その実行にユーザの許可が必要な機能を指定する指定工程と、プログラムから提示された機能一覧中に前記指定工程で指定された機能が含まれるか否かを判定する判定工程と、前記判定工程で前記機能一覧中に前記指定された機能が含まれると判定された場合に、前記プログラムをインストールするか否かをユーザに問い合わせる問い合わせ工程と、を含んだことを特徴とする。

【0020】この請求項4に記載の発明によれば、あらかじめ指定された処理をおこなうプログラムについては、インストールに先立ってユーザにその事実が警告されるとともに、ユーザが指示した場合には当該インストールが中止される。

【0021】また、請求項5に記載のプログラム実行防止方法は、その実行にユーザの許可が必要な機能を指定する指定工程と、プログラムから提示された機能一覧中に前記指定工程で指定された機能が含まれるか否かを判定する判定工程と、前記判定工程で前記機能一覧中に前記指定された機能が含まれると判定された場合に、前記プログラムを起動するか否かをユーザに問い合わせる問い合わせ工程と、を含んだことを特徴とする。

【0022】この請求項5に記載の発明によれば、あらかじめ指定された処理をおこなうプログラムについては、起動に先立ってユーザにその事実が警告されるとともに、ユーザが指示した場合には当該起動が中止される。

【0023】また、請求項6に記載のプログラム実行防止方法は、その実行にユーザの許可が必要な機能を指定する指定工程と、プログラムから呼び出された機能が前記指定工程で指定された機能であるか否かを判定する第1の判定工程と、前記第1の判定工程で前記呼び出された機能が前記指定された機能であると判定された場合に、前記呼び出された機能が前記プログラムから提示された機能一覧中に含まれていたか否かを判定する第2の判定工程と、前記第2の判定工程で前記呼び出された機能が前記プログラムから提示された機能一覧中に含まれていなかったと判定された場合に、前記プログラムの実行を継続するか否かをユーザに問い合わせる問い合わせ工程と、を含んだことを特徴とする。

【0024】この請求項6に記載の発明によれば、プログラムの実行中あらかじめ提示されたとは異なる機能が呼び出されたときは、ユーザにその事実が警告されるとともに、ユーザが指示した場合には当該プログラムの実行が中断される。

【0025】また、請求項7に記載のプログラムは、前記請求項4～請求項6のいずれか一つに記載の方法をフ

ンピュータに実行させるプログラムであることを特徴とする。

【0026】この請求項7に記載の発明によれば、前記請求項4～請求項6のいずれか一つに記載の方法がコンピュータにより読み取られて実行される。

【0027】また、請求項8に記載の記録媒体は、前記請求項7に記載のプログラムを記録したことを特徴とする。

【0028】この請求項8に記載の発明によれば、前記請求項7に記載の方法がコンピュータにより読み取られて実行される。

【0029】

【発明の実施の形態】以下に添付図面を参照して、この発明によるプログラム実行防止装置、プログラム実行防止方法、その方法をコンピュータに実行させるプログラムおよびそのプログラムを記録したコンピュータ読み取り可能な記録媒体の好適な実施の形態を詳細に説明する。

【0030】図1は、本発明の実施の形態にかかるプログラム実行防止装置のハードウェア構成を示す説明図である。同図において、101は装置全体を制御するCPUを、102は基本入出力プログラムを記憶したROMを、103はCPU101のワークエリアとして使用されるRAMを、それぞれ示している。

【0031】また、104はCPU101の制御にしたがってHD（ハードディスク）105に対するデータのリード/ライトを制御するHDD（ハードディスクドライバ）を、105はHDD104の制御にしたがって書き込まれたデータを記憶するHDを、それぞれ示している。また、106はCPU101の制御にしたがってFD（フロッピー（登録商標）ディスク）107に対するデータのリード/ライトを制御するFDD（フロッピーディスクドライバ）を、107はFDD106の制御にしたがって書き込まれたデータを記憶する着脱自在のFDを、それぞれ示している。

【0032】また、108はカーソル、メニュー、ウィンドウ、あるいは文字や画像などの各種データを表示するディスプレイを、109は通信ケーブル110を介してネットワークに接続され、当該ネットワークとCPU101とのインターフェースとして機能するネットワークインターフェースを、それぞれ示している。

【0033】また、111は文字、数値、各種指示などの入力のための複数のキーを備えたキーボードを、112は各種指示の選択や実行、処理対象の選択、カーソルの移動などをおこなうマウスを、それぞれ示している。また、113は着脱可能な記録媒体であるCD-ROMを、114はCD-ROM113に対するデータのリードを制御するCD-ROMドライバを、100は上記各部を接続するためのバスまたはケーブルを、それぞれ示している。

【0034】つぎに、図2は本発明の実施の形態にかかるプログラム実行防止装置の構成を機能的に示す説明図である。本発明によるプログラム実行防止装置は、具体的に(1)プラグインと、以下に説明するように

(2)当該プラグインの実行可否を判定し、実行可である場合に当該プラグインに各種機能(サービス)を提供するアプリケーション(ホストとなるアプリケーション)により実現される。そして、図2中200xはプラグインにより、201xはそのホストとなるアプリケーションにより、それぞれ実現される機能部である。

【0035】200aは、プラグインのインストール直前あるいは起動直前に、当該プラグインが使用する機能の一覧をそのホストとなるアプリケーションに提示する機能一覧提示部である。あるいは、ホストとのハンドシェイク時に、このプラグインが当該ホストから呼び出すことが予定されている機能の一覧を提示する、といってもよい。現実的には、インストールに先立っての機能提示は当該プラグインのインストールがおこなうことになる。

【0036】また、200bは所定の手続きにしたがって、ホストが提供する種々の機能(たとえばファイル読み込み、ファイル削除、ウィンドウ生成、テキスト出力などといったサービス)を呼び出し、各機能による処理をおこなわせる機能呼び出し部である。

【0037】つぎに、201aはプラグインの機能一覧提示部200aから提示された機能一覧を参照して、当該プラグインの実行前または実行中に、そのインストール可否や起動可否、あるいは継続可否(以下ではこれらをまとめて実行可否ともいう)を判定するセキュリティ管理部である。

【0038】また、201bはセキュリティ管理部201aによる判定の基礎となる、セキュリティポリシーを格納するセキュリティポリシーDB(データベース)である。このセキュリティポリシーには、(1)プラグインの実行前にその実行可否(インストール可否あるいは起動可否)を判定するためのものと、(2)プラグインの実行中にその実行可否(継続可否)を判定するためのものがある。

【0039】具体的には、(1)の実行前のセキュリティポリシーとは、「プラグインの実行前、当該プラグインから提示された機能一覧中に特定の機能が含まれている場合に、当該プラグインをインストールするか否か、あるいは起動するか否かをユーザに問い合わせる」というものであり、(2)の実行中のセキュリティポリシーとは、「プラグインの実行中、上記特定の機能であった、かつ当該プラグインから実行前に提示された機能一覧中にない機能が呼び出された場合に、当該プラグインの実行を継続するか否かをユーザに問い合わせる」というものである。

【0040】つぎに、201cは上記セキュリティポリシーの詳細設定をユーザから受け付けるとともに、設定された情報をセキュリティポリシーDB201bに格納するセキュリティポリシー設定部である。

【0041】図3は、セキュリティポリシー設定部201cにより表示される、上記(1)(2)のセキュリティポリシーの「特定の機能」を設定するための画面の一例を示す説明図である。図中左側のボックス300には、ホストとなるアプリケーションがそのプラグインに提供する機能のうち、ユーザやシステムにダメージを与えるおそれのあるものが列挙されている。

【0042】たとえばあるメーラーのプラグインが、ホストの機能呼び出すことで「別のプログラムが作成したファイルを削除できる」(図3参照)場合、当該プラグインの実行によって、システムファイルやその他のデータファイルがユーザの許可なく削除されてしまう可能性がある。これはシステムの異常・破壊や、メールがすべて消されてしまったなどの深刻な事態を引き起こしかねない。

【0043】また、プラグインが「別のプログラムを呼び出すことができる」場合、ホストが知らない別のプログラムが起動されてしまえば、以後はそのプログラムがどんな破壊的な行動をするか分からない。「レジストリにアクセスできる」場合、レジストリにはシステム情報や個人情報格納されているので、システムを破壊される。ダイアルアップの接続先を変えられる、個人情報(特にパスワード)を盗まれるなどの被害が発生する。

【0044】また、「アドレス帳に登録されていないユーザにメールを送ることができる」場合も、メールアドレスをはじめとするユーザの個人情報未知の相手に流出してしまう可能性がある。逆に、「アドレス帳に登録されているすべてのユーザにメールを送ることができる」場合も、昨春春に大流行した「I love you」の例から分かるように、知人から知人へ連鎖的にウィルスの被害が拡大するおそれがある。

【0045】なお、送信先はある程度多数であれば、必ずしもアドレス帳内の全ユーザでなくとも同様の危険がある(「Melissa」のように、最初の50件のアドレスへ自己の複製を送付するものもある)ので、ここは「すべて」の代わりに「〇人以上」などであってもよい。

【0046】また、アドレス帳内の全ユーザにメールを送信するとは、(1)アドレス帳からのメンバーの列挙と、(2)列挙したメンバーのメールの送信との二つの機能の組み合わせと見ることもできるので、上記の表現は「アドレス帳からメンバーを列挙してメールを送信することができる」などと言い換えることもできる。

【0047】ただし既知の相手であれ未知の相手であれ、メールの送信に生じるそのための送信先がユーザ

に示され、かつそのままの状態で（すなわち、本文の改ざんや新たなファイルの添付などがおこなわれず）送信されるならば危険はないと考えられるので、よりきめ細かに、上記からこうした例外的なケースを逐一除外するようにしてもよい。

【0048】図3に示す諸機能は常に上記のような危険をともなうものではなく、そのプラグインの目的上、当該機能を使用することが必要不可欠な場合もある。また、プラグインの目的と照らし合わせれば、ユーザが個々に危険性の有無を判断できる場合もある。たとえば、単にある形式の画像ファイルを表示させるためだけのプラグインであれば、明らかに他のファイルを削除する必要はなく、仮に当該プラグインがファイル削除の機能を呼び出している場合、何らかのウィルスに感染している可能性が高い。

【0049】そこで、図3の左側のボックス300に列挙する機能のうち、特に危険であって事前に確認が必要とユーザが考えるものだけを、右矢印ボタン301と左矢印ボタン302により右側のボックス303に抽出しておく。同図は上記特定の機能として、「アドレス帳に登録されているすべてのユーザにメールを送ることができ」を指定した例である。この状態でOKボタン304が押下されると、セキュリティポリシー設定部201cは設定内容をセキュリティポリシーDB201bに格納する。

【0050】図2に戻り、つぎに201dは実行可否問い合わせセ部であり、セキュリティ管理部201aがセキュリティポリシーDB201b内のセキュリティポリシーにもつぎ、ユーザの確認が必要と判定した場合に、その確認を得るためのダイアログを表示する。

【0051】図4は、実行可否問い合わせセ部201dにより表示される、プラグイン実行前にその実行可否を確認するためのダイアログの一例を示す説明図である。このダイアログには、プラグインが提示した機能一覧中、ユーザが図3の画面で指定した（左側のボックス300から右側のボックス303に抽出した、といってもよい）機能と一致するものが示されている。そして、このプラグインは図示するように、アドレス帳内の全ユーザへのメール送信という必ずしも安全とはいえない処理をおこなうが、それでも使用するかどうかユーザに問われている。

【0052】なお、図4のダイアログはプラグインの実行前であればいつ表示してもよいのであるが、現実的には（1）当該プラグインのインストール直前、および／または（2）当該プラグインの起動直前に表示することになる。

【0053】そして、インストール直前の確認でユーザが「はい」ボタン400を押下した場合、すなわち警告にもかかわらずユーザが当該プラグインの使用を許可した場合に、実行可否問い合わせセ部201dは次に図

5に示すようなダイアログを表示して、プラグインの起動直前にも再度同様の確認をおこなうかどうかを設定させた後、当該プラグインをインストールする。

【0054】なお、図4に示すダイアログでユーザが「いいえ」ボタン401を押下した場合には、インストールはおこなわずに、「プラグインのインストールを中止しました」などのメッセージを表示する。

【0055】また、図5に示すダイアログで「はい」ボタン500が押下された場合、すなわち起動直前にも確認をおこなうよう設定された場合には、この後インストールされたプラグインがそのホストから呼び出される都度、図4と同様のダイアログが表示されるようになる。

【0056】そして、起動直前に表示された同図のダイアログで「はい」ボタン400が押下された場合には、図5のダイアログを表示することなく当該プラグインを起動する。また、ここで「いいえ」ボタン401が押下されるとプラグインの起動はおこなわず、代わりに「プラグインを起動できません」などのメッセージを表示する。

【0057】また、図6は同じく実行可否問い合わせセ部201dにより表示される、プラグイン実行中にその実行可否を確認するためのダイアログの一例を示す説明図である。このダイアログはプラグインの実行中、ユーザが図3の画面で指定した機能であって、かつ実行前に提示された機能一覧中にない機能が呼び出されたときに随時表示される。

【0058】上述した（1）のセキュリティポリシーによる実行前（インストール直前あるいは起動直前）の確認だけでは、プラグインが偽装の機能一覧を提示するようなウィルスに感染した場合、危険な機能を申告しないことで容易に監視を逃れることができてしまう。そこで上述（2）のセキュリティポリシーにより、実行前に提示されたのと異なる機能が呼び出されていないかどうかを実行中でも常時監視するのである。

【0059】図6の例では、アドレス帳内の全ユーザへのメール送信は事前には申告されていないのであるが、当該プラグインの実行中、上記ダイアログの表示により上記機能の実行は一時保留され、いわば水際で食い止められることになる。

【0060】なお、図6のダイアログによる警告を受けたユーザは、問題ないと判断すれば「継続」ボタン600を押下することで、ダイアログで示された処理をそのまま実行させることができる。また、何らかの危険があると判断したときは、「中止」ボタン601を押下することでこのプラグインの実行をいったん中断し、プラグインの出所を再確認などの対策を取ることができる。

【0061】もっとも、事前に申告していない機能を呼び出すような怪しいプラグインは一切使用しないという方針であれば、「アンインストール」ボタン602を押

11

下することで、同図のダイアログから直接当該プラグインをアンインストールすることができる。

【0062】図2に戻り、つぎに201eはシステム保護部であり、プラグインの実行中その機能呼び出し部200bからいずれかの機能の呼び出しを受け付けると、セキュリティ管理部201aに対して、当該機能がユーザの確認なく実行を許可されるものであるかどうかを問い合わせる。

【0063】そして上述(2)のセキュリティポリシーのもとで実行が許可される場合、すなわち当該機能が事前に申告されたものである場合には、システム保護部201eは当該機能をプラグインに提供するいずれかの機能部(後述)に指示して、要求された処理をおこなわせる。

【0064】また、当該機能の実行が許可されない場合、すなわち当該機能が事前に申告されたものでない場合には、セキュリティ管理部201aからの指示を受けた実行可否問い合わせ部201dにより、図6に示したようなダイアログが表示される。そして、上述のようにこのダイアログで「継続」ボタン600が押下されたときに、システム保護部201eは上記機能をプラグインに提供するいずれかの機能部(後述)に指示して、要求された処理をおこなわせる。

【0065】図2に戻り、つぎに201f~201iはプラグインに対して各種の機能(サービス)を提供する機能部であり、201fはファイル読み込みのサービスを提供するファイル読み込み部、201gはファイル削除のサービスを提供するファイル削除部、201hはウィンドウ生成のサービスを提供するウィンドウ生成部、201iはテキスト出力のサービスを提供するテキスト出力部である。なお、提供される機能は上記に掲げたものの以外にも多数存在するが(たとえばレジストリアクセス、メール送信など)、同図では図示を省略している。

【0066】つぎに、図7~図9は本発明の実施の形態にかかるとプログラム実行防止システムにおける、プログラム実行防止処理の手順を示すフローチャートである。図7はプログラム(この場合はプラグイン)のインストールの中止、図8はプログラム(同左)の起動の中止、図9は実行中のプログラム(同左)の中断により、それぞれ結果的に危険なプログラムの実行を阻止するものである。

【0067】なお、同7~図9のフローチャートによる処理の開始に先立って、セキュリティポリシーDB201bにはセキュリティポリシー設定部201cにより、実行前および実行中のセキュリティポリシーがあらかじめ設定されているものとする。

【0068】まず図7に示す、インストールの中止によるプログラム実行防止の手順について説明する。プラグインの機能一覧提示部200aは、当該プラグインのインストールに先立って、その実行可能アプリケーション

12

ョンに対して、当該プラグインが呼び出して使用する機能の一覧を提示する(ステップS701)。

【0069】ホストとなるアプリケーションは、上記一覧をそのセキュリティ管理部201aで受領するとともに、セキュリティポリシーDB201b内のセキュリティポリシーを参照して、このプラグインのインストールにユーザの確認が必要かどうかを判定する(ステップS702)。具体的には、提示された一覧中にあらかじめ指定された機能が含まれるかどうかをチェックし、含まれていれば確認要、含まれていなければ確認不要とする。

【0070】そして、ユーザの確認が必要であれば(ステップS702:Yes)、実行可否問い合わせ部201dにより図4に示したようなダイアログを表示(ステップS703)、同図のダイアログで「はい」ボタン400が押下されたときは(ステップS704:Yes)、さらに図5に示したようなダイアログを表示する(ステップS705)。その後、当該プラグインのインストールを通常通りおこなって(ステップS706)、本フローチャートによる処理を終了する。

【0071】また、図4のダイアログで「いいえ」ボタン401が押下されたときは(ステップS704:No)、インストールをおこなう代わりに、インストールを中止した旨のメッセージを表示して(ステップS707)、本フローチャートによる処理を終了する。

【0072】つぎに図8に示す、起動の中止によるプログラム実行防止の手順について説明する。プラグインはそのホストとなるアプリケーションから呼び出されると、その機能一覧提示部200aにより、使用を予定している機能の一覧を提示する(ステップS801)。ホストではそのセキュリティ管理部201aにより、このプラグインの起動に先立ってユーザの確認が必要かどうかを判定する(ステップS802)。

【0073】具体的には、インストール時の図5のダイアログ(図7のステップS705)で、起動直前にも再度確認をおこなうように設定されている場合であって、かつ上記で提示された機能一覧中にあらかじめ指定された機能が含まれている場合に、ユーザの確認が必要と判定する(ステップS802:Yes)。そして実行可否問い合わせ部201dに指示して、図4に示したようなダイアログを表示させる(ステップS803)。

【0074】このダイアログで「はい」ボタン400が押下されると(ステップS804:Yes)、プラグインを通常通り起動し(ステップS805)、「いいえ」ボタン401が押下されると(ステップS804:No)、プラグインの起動を中止した旨のメッセージを表示(ステップS806)した後、本フローチャートによる処理を終了する。

【0075】つぎに図9に示す、実行中断によるプログラム実行防止の手順について説明する。プラグインの機

能呼び出し部 200b から、そのホストとなるアプリケーションに対して機能の呼び出しがあると（ステップ S901）、システム保護部 201e はセキュリティ管理部 201a に指示して、当該機能がユーザの確認なく実行してもよいものであるかどうかを判定させる（ステップ S902）。

【0076】セキュリティ管理部 201a は、当該機能がセキュリティポリシー設定部 201c によりあらかじめ指定された機能であって、かつ実行前（インストール直前および／または起動直前）に提示された機能と異なる場合にユーザの確認が必要と判定し（ステップ S902：Yes）、実行可否問い合わせ部 201d に指示して、図 6 に示したようなダイアログを表示させる（ステップ S903）。

【0077】そして、このダイアログで「継続」ボタン 600 が押下されると（ステップ S904：Yes）呼び出された処理を実行する、すなわちプラグインの実行をそのまま継続し（ステップ S905）、「中止」ボタン 601 が押下されると（ステップ S904：No、ステップ S906：Yes）、その時点でプラグインの実行を中断するとともにその事実をメッセージにより表示する（ステップ S907）。

【0078】また、「アンインストール」ボタン 602 が押下されると（ステップ S906：No）、当該プラグインをアンインストール（ステップ S908）した後、本フローチャートによる処理を終了する。

【0079】なお、上述した実施の形態ではユーザの指示を待ってインストール中止、起動中止あるいは実行中断などをおこなったが、あるいは提示された機能一覧中にあらかじめ指定した機能が含まれていた時点で、あらかじめ提示された機能一覧中にない機能が呼び出された時点で、ユーザの指示を待たず強制的に中止や中断をおこなうようにしてもよい。

【0080】また、上述した実施の形態ではプログラムが使用する機能単位でユーザに確認するかしないかの設定をおこなったが（図 3）、あるいはプログラムごとに確認するかしないかを設定できるようにしてもよい。たとえば一つの PC を複数人で使用している場合、他の使用者により危険なプラグイン（出所の定かでないプラグインなど）が安易に導入されることのないように、管理責任者があらかじめプラグインを指定しておき、それ以外のプラグインがインストールされそうになったときに図 4 のような警告を表示するようにしてもよい。

【0081】なお、上述の各機能部を実現するプログラムは、HD105 のほか FD107、CD-ROM113 あるいは MO などの各種記録媒体に格納することができ、当該記録媒体によって配布することができる。また、ネットワークを介して配布することも可能である。

【0082】なお、上記説明からも明らかなように、図 2 に示すセキュリティ管理部 201a の構成位置にいう

「判定手段」「第 1 の判定手段」および「第 2 の判定手段」に相当し、そのおこなう処理が請求項にいう「判定工程」「第 1 の判定工程」および「第 2 の判定工程」に相当する。

【0083】また、セキュリティポリシー設定部 201c が請求項にいう「指定手段」に、そのおこなう処理が請求項にいう「指定工程」に相当する。さらに、実行可否問い合わせ部 201d が請求項にいう「問い合わせ手段」に、そのおこなう処理が請求項にいう「問い合わせ工程」に相当する。

【0084】以上説明したように本発明の実施の形態によれば、ユーザやシステムにダメージを与えるおそれのある機能がプラグイン中に含まれる場合に、ユーザの判断にしたがって当該プラグインのインストールや起動が拒否されるので、当該プラグインが実行された結果生ずるかもしれない損害を未然に回避することができる。

【0085】また、実行前に提示された機能一覧を安易に信用することなく、実行中にもその信憑性を常時監視しているため、事前に申告していない危険な機能を実行中にひそかに呼び出そうとするようなプラグインを、当該機能が呼び出される直前に停止させることができる。これによりもたらされる効果は上記と同様である。

【0086】そして、本発明はその原理上、ウィルスに感染したプログラムであるか何らかの悪意をもって作成されたプログラムであるかを問わず、ユーザやシステムにとって危険な動作をするものであればその実行を阻止することができるので、従来技術で指摘困難だった、通常のプログラムと区別つかない悪意のあるプログラムも容易に検出することができる。

【0087】また、近年増加している多形態型のウィルスであっても、その目的とする処理が同一である限り、表面的なコードの差異にかかわらず検出できるという特長を持っている。しかもその検出のために、すべてのウィルスのコード群を網羅したウィルス定義ファイル（パターンファイル、DAT ファイルなどという）を用意する必要はなく、また当該ファイルを頻繁に更新する作業も不要である。

【0088】また、本発明は上述のように、呼び出し予定の機能の中に危険なものが含まれるか、実際に呼び出された機能が事前に申告されていたかといった、ごく単純な判定によりプログラムの実行を阻止すること、従来のウィルススキャンのように長時間を要することなく、日々無理なく励行され実効性ははかれるという現実的なメリットもある。

【0089】また、従来技術の Java のように使用できる機能を一律に制限するものではないので、プログラムの自由度が増し、安全性と利便性の両立をはかることが可能である。

【0090】なお、上述した実施の形態ではプログラムの中にあるプラグインについて、そのホストとなるア

プリケーションにおいて実行可否を判定するようにしたが、たとえばマクロと当該マクロの動作するアプリケーションとの関係に本発明を応用することも可能である。

【0091】また、一般のアプリケーションとOSとの間に本発明を適用する、すなわちOSそのものにプログラムのインストールの中止や起動の中止、あるいは実行中のプログラムの中断の機能を持たせることもできる。これにより、別途アンチウイルスソフトなどを導入すること等、あるいはそれ以上の危険防止効果が得られることになる。

【0092】図10は、本発明によるプログラム実行防止機能をOSに具備させた場合に、アプリケーションの実行がどのように阻止されるかを模式的に示す説明図である。同図は偽装の機能一覧の提示により、いったんインストールおよび起動を許可されたアプリケーションが、実行中に上記一覧中ない、ファイル削除機能を出した時点で中断される例を示している。

【0093】

【発明の効果】以上説明したように請求項1に記載の発明は、その実行にユーザの許可が必要な機能を指定する指定手段と、プログラムから提示された機能一覧中に前記指定手段により指定された機能が含まれるか否かを判定する判定手段と、前記判定手段により前記機能一覧中に前記指定された機能が含まれると判定された場合に、前記プログラムをインストールするか否かをユーザに問い合わせる問い合わせ手段と、を備えたので、あらかじめ指定された処理をおこなうプログラムについては、インストールに先立ってユーザにその事実が警告されるとともに、ユーザが指示した場合には当該インストールが中止され、これによって、ユーザやシステムにとって危険なプログラムの実行を未然に防止することが可能なプログラム実行防止装置が得られるという効果を奏する。

【0094】また、請求項2に記載の発明は、その実行にユーザの許可が必要な機能を指定する指定手段と、プログラムから提示された機能一覧中に前記指定手段により指定された機能が含まれるか否かを判定する判定手段と、前記判定手段により前記機能一覧中に前記指定された機能が含まれると判定された場合に、前記プログラムを起動するか否かをユーザに問い合わせる問い合わせ手段と、を備えたので、あらかじめ指定された処理をおこなうプログラムについては、起動に先立ってユーザにその事実が警告されるとともに、ユーザが指示した場合には当該起動が中止され、これによって、ユーザやシステムにとって危険なプログラムの実行を未然に防止することが可能なプログラム実行防止装置が得られるという効果を奏する。

【0095】また、請求項3に記載の発明は、その実行にユーザの許可が必要な機能を指定する指定手段と、プログラムから呼び出された機能が前記指定手段により指定された機能であるか否かを判定する第1の判定手段

と、前記第1の判定手段により前記呼び出された機能が前記指定された機能であると判定された場合に、前記呼び出された機能が前記プログラムから提示された機能一覧中に含まれていたか否かを判定する第2の判定手段と、前記第2の判定手段により前記呼び出された機能が前記プログラムから提示された機能一覧中に含まれていなかったと判定された場合に、前記プログラムの実行を継続するか否かをユーザに問い合わせる問い合わせ手段と、を備えたので、プログラムの実行中あらかじめ提示されたのとは異なる機能が呼び出されたときは、ユーザにその事実が警告されるとともに、ユーザが指示した場合には当該プログラムの実行が中断され、これによって、ユーザやシステムにとって危険なプログラムの問題部分の実行を未然に防止することが可能なプログラム実行防止装置が得られるという効果を奏する。

【0096】また、請求項4に記載の発明は、その実行にユーザの許可が必要な機能を指定する指定工程と、プログラムから提示された機能一覧中に前記指定工程で指定された機能が含まれるか否かを判定する判定工程と、前記判定工程で前記機能一覧中に前記指定された機能が含まれると判定された場合に、前記プログラムをインストールするか否かをユーザに問い合わせる問い合わせ工程と、を含んだので、あらかじめ指定された処理をおこなうプログラムについては、インストールに先立ってユーザにその事実が警告されるとともに、ユーザが指示した場合には当該インストールが中止され、これによって、ユーザやシステムにとって危険なプログラムの実行を未然に防止することが可能なプログラム実行防止装置が得られるという効果を奏する。

【0097】また、請求項5に記載の発明は、その実行にユーザの許可が必要な機能を指定する指定工程と、プログラムから提示された機能一覧中に前記指定工程で指定された機能が含まれるか否かを判定する判定工程と、前記判定工程で前記機能一覧中に前記指定された機能が含まれると判定された場合に、前記プログラムを起動するか否かをユーザに問い合わせる問い合わせ工程と、を含んだので、あらかじめ指定された処理をおこなうプログラムについては、起動に先立ってユーザにその事実が警告されるとともに、ユーザが指示した場合には当該起動が中止され、これによって、ユーザやシステムにとって危険なプログラムの実行を未然に防止することが可能なプログラム実行防止装置が得られるという効果を奏する。

【0098】また、請求項6に記載の発明は、その実行にユーザの許可が必要な機能を指定する指定工程と、プログラムから呼び出された機能が前記指定工程で指定された機能であるか否かを判定する第1の判定工程と、前記第1の判定工程で前記呼び出された機能が前記指定された機能であると判定された場合に、前記呼び出された機能が前記プログラムから提示された機能一覧中に含

れていたか否かを判定する第2の判定工程と、前記第2の判定工程で前記呼び出された機能が前記プログラムから提示された機能一覧中に含まれていなかったと判定された場合に、前記プログラムの実行を継続するか否かをユーザに問い合わせる問い合わせ工程と、を含んだので、プログラムの実行中あらかじめ提示されたのとは異なる機能が呼び出されたときは、ユーザにその事実が警告されるとともに、ユーザが指示した場合には当該プログラムの実行が中断され、これによって、ユーザやシステムにとって危険なプログラムの問題部分の実行を未然に防止することが可能なプログラム実行防止方法が得られるという効果を奏する。

【0099】また、請求項7に記載の発明は、前記請求項4～請求項6のいずれか一つに記載の方法をコンピュータに実行させるので、前記請求項4～請求項6のいずれか一つに記載の方法がコンピュータにより読み取られて実行され、これによって、ユーザやシステムにとって危険なプログラム、あるいは少なくともその問題部分の実行を未然に防止することが可能なプログラムが得られるという効果を奏する。

【0100】また、請求項8に記載の発明は、前記請求項7に記載のプログラムを記録したので、前記請求項7に記載のプログラムがコンピュータにより読み取られて実行され、これによって、ユーザやシステムにとって危険なプログラム、あるいは少なくともその問題部分の実行を未然に防止することが可能な記録媒体が得られるという効果を奏する。

【図面の簡単な説明】

【図1】本発明の実施の形態にかかるプログラム実行防止装置のハードウェア構成を示す説明図である。

【図2】本発明の実施の形態にかかるプログラム実行防止装置の構成を機能的に示す説明図である。

【図3】セキュリティポリシー設定部201cにより表示される、セキュリティポリシーの詳細を設定するための画面の一例を示す説明図である。

【図4】実行可否問い合わせ部201dにより表示される、プラグイン実行前にその実行可否を確認するためのダイアログの一例を示す説明図である。

【図5】実行可否問い合わせ部201dにより表示される、プラグインの起動直前にも実行可否を確認するかどうかを設定するためのダイアログの一例を示す説明図である。

【図6】実行可否問い合わせ部201dにより表示される、プラグイン実行中にその実行可否を確認するためのダイアログの一例を示す説明図である。

【図7】本発明の実施の形態にかかるプログラム実行防止システムにおける、インストールの中止によるプログラム実行防止処理の手順を示すフローチャートである。

【図8】本発明の実施の形態にかかるプログラム実行防止システムにおける、起動中止によるプログラム実行防止処理の手順を示すフローチャートである。

【図9】本発明の実施の形態にかかるプログラム実行防止システムにおける、実行中断によるプログラム実行防止処理の手順を示すフローチャートである。

【図10】本発明をOSに応用した場合にアプリケーションの実行がどのように阻止されるかを模式的に示す説明図である。

【符号の説明】

100 バスまたはケーブル

101 CPU

102 ROM

103 RAM

104 HDD

105 HD

106 FDD

107 FD

108 ディスプレイ

109 ネットワーク I/F

110 通信ケーブル

111 キーボード

112 マウス

113 CD-ROM

114 CD-ROMドライブ

200a 機能一覧提示部

200b 機能呼び出し部

201a セキュリティ管理部

201b セキュリティポリシーDB

201c セキュリティポリシー設定部

201d 実行可否問い合わせ部

201e システム保護部

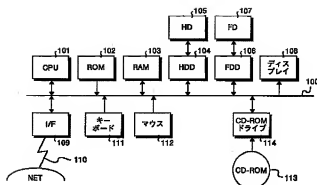
201f ファイル読み込み部

201g ファイル削除部

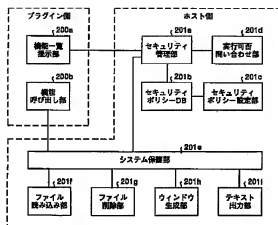
201h ウィンドウ生成部

201i テキスト出力部

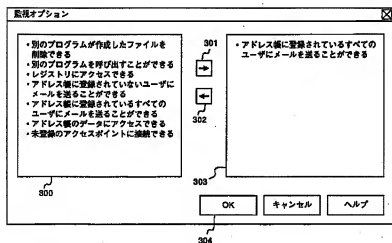
【図1】



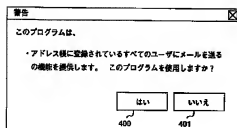
【図2】



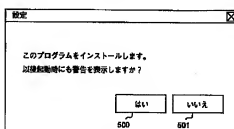
【図3】



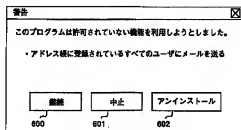
【図4】



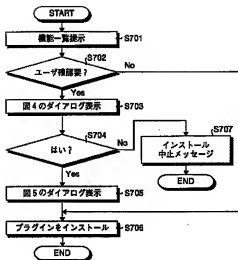
【図5】



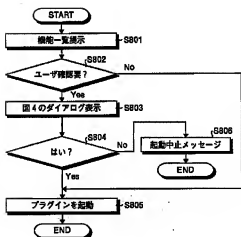
【図6】



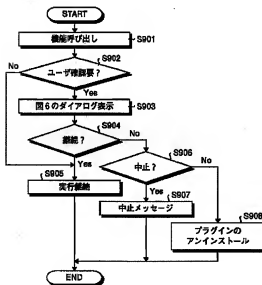
【図7】



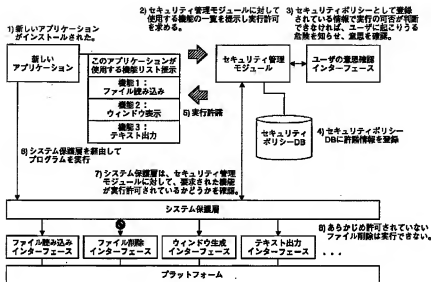
【図8】



【図9】



【図10】



PATENT ABSTRACTS OF JAPAN

(11)Publication number : 2003-067210

(43)Date of publication of application : 07.03.2003

(51)Int.Cl.

G06F 11/00

(21)Application number : 2001-251925 (71)Applicant : JUST SYST CORP

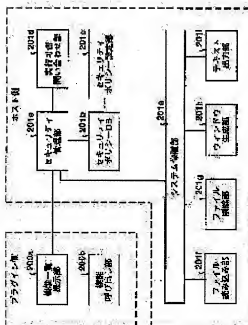
(22)Date of filing : 22.08.2001 (72)Inventor : TOYODA MITSUKI

(54) PROGRAM EXECUTION PREVENTION DEVICE, PROGRAM EXECUTION PREVENTION METHOD, PROGRAM FOR COMPUTER TO EXECUTE THE METHOD, AND COMPUTER READABLE RECORDING MEDIUM STORED WITH THE PROGRAM

(57)Abstract:

PROBLEM TO BE SOLVED: To prevent the execution of a program dangerous to a user and a system, such as a virus infected program and a maliciously created program.

SOLUTION: Prior to installation or starting up of a plug-in, a function list showing unit 200a thereof shows to an application to be a host a list of functions (services) to be used by acquiring from the host. When a dangerous function (erasing a file, etc.), specified in advance in the list is included, a security management unit 201a of the host asks the user whether or not to still continue the installation/starting-up by an execution inquiry



unit 201d. Also, during a plug-in execution, whether or not to continue the execution of the plug-in is inquired at any time when an actually requested function is not shown in the above list.

DETAILED DESCRIPTION

[Detailed Description of the Invention]

[0001]

[Field of the Invention]This invention relates to the recording medium which recorded the program which makes a computer perform the program execution arrester which prevents beforehand execution of a program dangerous for a user or a system, a program execution prevention method, and its method, and its program and in which computer reading is possible.

[0002]

[Description of the Prior Art]Although maintenance of the network (LAN) which connects the computer of the premises mutually from early was progressing in large-scale organisms, such as a company and a university, Since the client/server system of a PC base can introduce easily and cheaply, also at small and medium-sized enterprises, an individual home, etc., the network of two or more of the computers to hold is progressing quickly in recent years.

[0003]The computer has become rather more common [being used accessing the Internet] rather than being used by a stand-alone by explosive expansion of the Internet for the past several years. Connection also becomes less new and not only the number of the computer connected to the Internet but the connect time of each computer is always in the tendency which increases increasingly these days.

[0004]However, the data exchange with other computers in a network is one side of the convenience, and is also providing the opportunity of capital growth to the computer virus which invaded into the network concerned. The "I love you" virus (correctly worm) which spread in May, last year all over the world spreads, while winking through the e-mail system of the Internet, and the total amount of the material and immaterial damage which this generated measures, and is not found.

[0005]

[Problem(s) to be Solved by the Invention]And in order to avoid generating of the damage caused by such a virus beforehand, the software for virus detection and extermination is also marketed, but. The detection and extermination by this were surely "followed" on the principle, and there were problems, such as that it cannot respond and becoming a "pinching game" with a new type of virus which it is developed one after another and made skillful, in a strange virus.

[0006]In such software, namely, a boot sector, a system memory, A partition table, a file,

etc. check the existence of a code group (pattern) peculiar to a specific virus about all the possible places of a viral infection, and a virus is specified from the discovered code group.

[0007]The virus which is not all over the table which matched a virus and its peculiar code group since it is such a principle, For example, even if it is a known virus as well as the strange virus which is not discovered and analyzed once until now, when the user has neglected renewal of a table, it cannot detect and exterminate.

[0008]Although the pleiomorphia type virus which gets used even to which of the gestalt of 4 billion is increasing since the release of Mutation Engine (software with which a simple virus is easily changed into the maker of a virus by the pleiomorphia type), Since the code group contained in this type of virus is changing from the original thing, the detection and extermination by the above-mentioned technique become difficult.

[0009]Furthermore, the above-mentioned software is a thing aiming at detection and extermination of a virus chiefly, In that a damage is given, it has the essential problem that a program with a certain bad faith without a virus and great difference is undistinguishable from the program which is not so in the user or the system. For example, unless all ActiveX controls which change a dialup place freely, and programs prepared in order to automate setting out and change of a dialup place are infected with the virus, execution will be permitted similarly.

[0010]There are some which have restricted access to a local resource based on the security policy for every environment of that depending on this point environment. For example, the Java applets (i application etc.) performed on VM of Java cannot access the files (for example, telephone directory etc.) on the computer which operates at all.

[0011]From a viewpoint of safety, this is a very powerful and positive defense method, but on the other hand it serves as big obstacle and restriction in development of practical application, and there is a problem that the convenience of a developer or a user is spoiled.

[0012]A program with this invention dangerous for a user or a system, or a program execution arrester which can prevent execution of that problem portion beforehand at least, It aims at providing the recording medium which recorded the program which makes a computer perform a program execution prevention method and its method, and its program and in which computer reading is possible.

[0013]

[Means for Solving the Problem]In order to solve a technical problem mentioned above and to attain the purpose, a program execution arrester concerning the invention according to claim 1 is provided with the following.

A setting means to which a user's permission specifies a required function as the execution.

A judging means which judges whether a function specified by said setting means in a functional listing shown from a program is included.

An inquiring means which asks a user whether install said program when judged with said specified function being included by said judging means in said functional listing.

[0014]According to this invention according to claim 1, about a program which performs processing specified beforehand, while being warned to a user of that fact in advance of installation, when a user points, the installation concerned is stopped.

[0015]The program execution arrester according to claim 2 is provided with the following.

A setting means to which a user's permission specifies a required function as the execution.

A judging means which judges whether a function specified by said setting means in a functional listing shown from a program is included.

An inquiring means which asks a user whether start said program when judged with said specified function being included by said judging means in said functional listing.

[0016]According to this invention according to claim 2, about a program which performs processing specified beforehand, while being warned to a user of that fact in advance of starting, when a user points, the starting concerned is stopped.

[0017]The program execution arrester according to claim 3 is provided with the following.

A setting means to which a user's permission specifies a required function as the execution.

The 1st judging means that judges whether a function called from a program is a function specified by said setting means.

The 2nd judging means that judges whether it was contained in a functional listing shown said called function from said program when judged with said called function being said specified function by said 1st judging means, An inquiring means which asks a user whether continue execution of said program when judged with not having been contained in a functional listing shown said called function from said program by said 2nd judging means.

[0018]According to this invention according to claim 3, when a different function from

having been beforehand shown during execution of a program is called, while being warned to a user of that fact, when a user points, execution of the program concerned is interrupted.

[0019]The program execution prevention method according to claim 4, A determination process which judges whether a function specified at said specification process is included in a specification process to which a user's permission specifies a required function as the execution, and a functional listing shown from a program, When judged with said specified function being included in said functional listing by said determination process, an inquiry process of asking a user whether install said program was included.

[0020]According to this invention according to claim 4, about a program which performs processing specified beforehand, while being warned to a user of that fact in advance of installation, when a user points, the installation concerned is stopped.

[0021]The program execution prevention method according to claim 5, A determination process which judges whether a function specified at said specification process is included in a specification process to which a user's permission specifies a required function as the execution, and a functional listing shown from a program, When judged with said specified function being included in said functional listing by said determination process, an inquiry process of asking a user whether start said program was included.

[0022]According to this invention according to claim 5, about a program which performs processing specified beforehand, while being warned to a user of that fact in advance of starting, when a user points, the starting concerned is stopped.

[0023]The program execution prevention method according to claim 6, A specification process to which a user's permission specifies a required function as the execution, and the 1st determination process that judges whether a function called from a program is a function specified at said specification process, The 2nd determination process that judges whether it was contained in a functional listing shown said called function from said program when judged with said called function being said specified function by said 1st determination process, When it judged that it was not contained by said called function in a functional listing shown from said program by said 2nd determination process, an inquiry process of asking a user whether continue execution of said program was included.

[0024]According to this invention according to claim 6, when a different function from having been beforehand shown during execution of a program is called, while being warned to a user of that fact, when a user points, execution of the program concerned is

interrupted.

[0025]The program according to claim 7 is characterized by being a program which makes a computer perform a method of any one statement of said claim 4 - claim 6.

[0026]According to this invention according to claim 7, a method of any one statement of said claim 4 - claim 6 is read by computer, and is performed.

[0027]The recording medium according to claim 8 recorded said program according to claim 7.

[0028]According to this invention according to claim 8, said method according to claim 7 is read by computer, and is performed.

[0029]

[Embodiment of the Invention]With reference to an accompanying drawing, the suitable embodiment of the recording medium which recorded the program which makes a computer perform the program execution arrester by this invention, a program execution prevention method, and its method, and its program and in which computer reading is possible is described in detail below.

[0030]Drawing 1 is an explanatory view showing the hardware constitutions of the program execution arrester concerning an embodiment of the invention. In the figure, RAM for which 103 are used as a work area of CPU101 in ROM 102 remembered the intercalation output program to be for CPU by which 101 controls the whole device is shown, respectively.

[0031]HD which memorizes the data in which HDD (hard disk drive) by which 104 controls the read/write of the data to HD(hard disk) 105 according to control of CPU101 was written in 105 according to control of HDD104 is shown, respectively. 106 FDD (floppy disk drive) which controls the read/write of the data to FD(floppy (registered trademark) disk) 107 according to control of CPU101, 107 shows FD which can be detached and attached and which memorizes the data written in according to control of FDD106, respectively.

[0032]The display on which 108 displays various data, such as cursor, a menu, a window or a character, and a picture, It is connected to a network via the telecommunication cable 110, and 109 shows the network interface which functions as an interface of the network concerned and CPU101, respectively.

[0033]The mouse in which 112 performs the keyboard with which 111 was provided with two or more keys for inputs, such as a character, a numerical value, and various directions, for selection of various directions, execution and selection of a processing object, movement of cursor, etc. is shown, respectively. A bus or a cable for 100 to connect each part of the above for the CD-ROM drive with which 114 control the lead of

data [as opposed to CD-ROM113 for CD-ROM whose 113 is a removable recording medium] is shown, respectively.

[0034]Next, drawing 2 is an explanatory view showing functionally the composition of the program execution arrester concerning an embodiment of the invention. The program execution arrester by this invention specifically (1) plug-in, it explains below -- as -- (2) -- the execution propriety of the plug-in concerned is judged, and when execution is good, it realizes more, without the application (application which serves as a host) which provides the plug-in concerned with a various function (service). And the inside 200x of drawing 2 is a function part realized with plug-in by the application with which 201x becomes the host, respectively.

[0035]200a is a functional listing presentation part which shows the application which serves as the host the list of the functions which the plug-in concerned uses just before installation of plug-in, or starting. Or at the time of a handshake with a host, the list of the functions in which it is planned that this plug-in calls from the host concerned is shown, but it is good. Actually, the installer of the plug-in concerned will perform functional presentation before installation, and the main part of the plug-in concerned will perform functional presentation before starting after installation.

[0036]200b is a function call part in which call various functions (for example, services, such as file reading, file deletion, window generation, and a text output) which a host provides according to a predetermined procedure, and processing by each function is made to perform.

[0037]Next, 201a refers to the functional listing shown from the functional listing presentation part 200a of plug-in. It is a security management department which judges the installation propriety and starting propriety, or continuation propriety (these are also collectively called execution propriety below) before execution of the plug-in concerned, or during execution.

[0038]201b is the security policy DB (database) used as the foundation of the judgment by the security management department 201a which stores a security policy. There are a thing for judging that execution propriety (installation propriety or starting propriety) before execution of (1) plug-in and a thing for judging that execution propriety (continuation propriety) during execution of (2) plug-in in this security policy.

[0039]Specifically with the security policy before execution of (1). "when the specific function is included in the functional listing shown from the plug-in concerned before execution of plug-in, Say whether install the plug-in concerned and that it asks a user whether start or not", and with the security policy under execution of (2). "When the function which is not into the functional listing which is the above-mentioned specific

function during execution of plug-in, and was shown before execution from the plug-in concerned is called, it asks a user whether continue execution of the plug-in concerned."

[0040]Next, 201c is a security policy set part which stores the set-up information in security policy DB201b while receiving the detailed setting of the above-mentioned security policy from a user.

[0041]Drawing 3 is an explanatory view which is displayed by the security policy set part 201c and in which showing an example of the screen for setting up "the specific function" of the security policy of the above (1) and (2). What has a possibility of giving a damage to a user and a system among the functions with which the application which serves as a host provides the plug-in in the box 300 of the left-hand side in a figure is enumerated.

[0042]For example, as for a "deleting file which another program created" (refer to drawing 3)-by calling host's function case, a system file and other data files may be deleted without a user's permission by execution of the plug-in concerned. [plug-in of a certain mailer] This may cause the serious situations -- all of the abnormalities and destruction of a system, and mail have been erased.

[0043]If another program in which a host does not have a concern will be started when plug-in "can call another program", there is no telling what kind of destructive action the program carries out henceforth. Since system information and personal information are stored in registry when "registry can be accessed", damage -- the personal information (especially password) which can change the connection destination of the dialup which has a system destroyed is stolen -- may occur.

[0044]Also when "e-mail can be sent to the user who is not registered into an address book", the personal information of users including a mail address may flow into a strange partner. On the contrary, also when "e-mail can be sent to all the users registered into the address book", there is a possibility that the damage of a virus may be continuously expanded from an acquaintance to an acquaintance so that the example of "I love you" which was much in fashion in the spring of last year may show.

[0045]in addition -- if transmission destinations are a large number to some extent, they are that which has the same danger even if it is not necessarily All Users in an address book (there are some which send a self duplicate to the first address of 50 affairs like "Melissa") -- here -- "all" -- it may be "more than O people" etc. instead.

[0046]transmitting e-mail to All Users in an address book, (1) Since it can also regard as the combination of two functions of listing of Memba from an address book, and transmission of the mail to Memba which carried out (2) listings, the above-mentioned expression can also be put in another way as "Memba can be enumerated from an

address book and e-mail can be transmitted" etc.

[0047]however, a known partner -- be -- a strange partner -- be -- the text and transmission destination being shown to a user and in advance of transmission of e-mail, And since it will be thought that there is no danger if transmitted in the state as it is (namely, ** to which neither alteration of the text nor attachment of a new file is performed), it may be made to except such an exceptional case from the above in detail more finely.

[0048]Many functions shown in drawing 3 may not be accompanied by the always above danger, and it may be indispensable on the purpose of the plug-in to use the function concerned. If it refers to the purpose of plug-in, a user may be able to judge the existence of danger separately. For example, if it is plug-in only for only displaying the graphics file of a certain form, when it is not necessary to delete other files clearly and the plug-in concerned is calling the function of file deletion temporarily, a possibility of being infected with a certain virus is high.

[0049]Then, among the functions to enumerate in the box 300 on the left-hand side of drawing 3, it is dangerous and the check extracts especially only what necessity and a user consider in the right-hand side box 303 with the right arrow button 301 and the left arrow button 302 a priori. As the above-mentioned specific function, the figure is the example which specified "e-mail can be sent to all the users registered into the address book." If OK button 304 is pushed in this state, the security policy set part 201c stores a setting detail in security policy DB201b.

[0050]It returns to drawing 2, and next, it is an execution propriety inquiry part, and 201 d displays the dialog for obtaining the check, when the security management department 201a judges with a user's check being required based on the security policy in security policy DB201b.

[0051]Drawing 4 is an explanatory view showing an example of the dialog for checking the execution propriety before plug-in execution displayed by the execution propriety inquiry part 201d. The function (it extracted from the left-hand side box 300 in the right-hand side box 303, but is good) and match which the user specified on the screen of drawing 3 are shown in this dialog among the functional listing which plug-in presented. And processing which is called the transmitting mail to All Users in an address book and which cannot necessarily be said as safety is performed so that this plug-in may be illustrated, but the user is asked about whether it is still used.

[0052]in addition -- although the dialog of drawing 4 may be displayed any time as long as it is before execution of plug-in -- realistic -- (1) -- just before installation of the plug-in concerned, and/or (2) -- it will display just before starting of the plug-in

concerned.

[0053]And when a user pushes the "yes" button 400 by the check in front of installation (i.e., when a user permits use of the plug-in concerned in spite of warning). The execution propriety inquiry part 201d displays a dialog as further shown in drawing 5, and after making it set up whether the check again same also just before starting of plug-in is performed, it installs the plug-in concerned.

[0054]When a user pushes the "no" button 401 in the dialog shown in drawing 4, installation displays the message of "having stopped installation of plug-in", without carrying out.

[0055]When the "yes" button 500 is pushed in the dialog shown in drawing 5 (i.e., when set up also check just before starting), whenever plug-in installed after this is called by that host, the same dialog as drawing 4 comes to be displayed.

[0056]And when the "yes" button 400 is pushed in the dialog of the figure displayed just before starting, the plug-in concerned is started, without displaying the dialog of drawing 5. If the "no" button 401 is pushed here, starting of plug-in will not be performed but will display the message of "were not able to start plug-in" instead.

[0057]Drawing 6 is an explanatory view showing an example of the dialog for checking the execution propriety during plug-in execution similarly displayed by the execution propriety inquiry part 201d. This dialog is displayed at any time, when the function which is not into the functional listing which is the function which the user specified on the screen of drawing 3 during execution of plug-in, and was shown before execution is called.

[0058]Only by the check before the execution by the security policy of (1) mentioned above (just before installation or starting), when plug-in is infected with the virus which can present the functional listing of camouflage, surveillance will be able to be easily escaped by not notifying a dangerous function. Then, also while performing whether the function which differs from having been shown before execution by the above-mentioned (2) security policy is called, it monitors continuously.

[0059]In the example of drawing 6, although the transmitting mail to All Users in an address book was not notified a priori, execution of the above-mentioned function will be suspended by the display of the above-mentioned dialog during execution of the plug-in concerned temporarily, and, so to speak, it will be stopped at the water's edge.

[0060]The user who received the warning by the dialog of drawing 6 can perform processing shown in the dialog as it is by carrying out the depression of the "continuation" button 600, if it judges that it is satisfactory. When it judges that there is a certain danger, execution of this plug-in can once be interrupted for carrying out the

depression of the "stop" button 601, and the measures against reconfirming the source of plug-in etc. can be taken.

[0061]But if it is planned to say that no doubtful plug-in which calls the function which has not been notified a priori is used, the plug-in concerned is uninstallable from directly the dialog of the figure by carrying out the depression of the "uninstallation" button 602.

[0062]If it returns to drawing 2, then 201e is a system-protection part and the call of one of functions is received from the function call part 200b during execution of plug-in. It is asked to the security management department 201a whether the function concerned is what execution is permitted without an user validation.

[0063]And when execution is permitted under the above-mentioned (2) security policy (i.e., when the function concerned is notified a priori), it points to the system-protection part 201e to one which provides plug-in with the function concerned of function parts (after-mentioned), and it makes the demanded processing perform.

[0064]When execution of the function concerned is not permitted (i.e., when the function concerned is not what was notified a priori), a dialog as shown in drawing 6 is displayed by the execution propriety inquiry part 201d which received the directions from the security management department 201a. And when "continuation" button 600 is pushed in this dialog as mentioned above, it points to the system-protection part 201e to one which provides plug-in with the above-mentioned function of function parts (after-mentioned), and it makes the demanded processing perform.

[0065]It returns to drawing 2 and then 201f-201i are function parts which provide various kinds of functions (service) to plug-in. The file reading part which provides 201 f of services of file reading, The file deletion part which provides 201 g of service of file deletion, the window generation part which provides 201 h of services of window generation, and 201i are text outputting parts which provide service of a text output. Although many functions provided exist besides what was hung up above, the graphic display is omitted in the figure (for example, registry access, transmitting mail, etc.).

[0066]Next, drawing 7 - drawing 9 are flow charts in the program execution prevention system concerning an embodiment of the invention which show the procedure of a program execution preventing process. Drawing 7 prevents the stop of installation of a program (in this case, plug-in), drawing 8 prevents the stop of starting of a program (the left), and drawing 9 prevents execution of a program respectively dangerous as a result by discontinuation of the program (the left) under execution.

[0067]In advance of the start of processing by the flow chart of the 7- drawing 9, the security policy before execution and under execution shall be beforehand set as security

policy DB201b by the security policy set part 201c.

[0068]The procedure of the prevention from program execution by the stop of installation first shown in drawing 7 is explained. The functional listing presentation part 200a of plug-in presents the list of the functions which the plug-in concerned calls and uses in advance of installation of the plug-in concerned to the application which serves as the host (Step S701).

[0069]It is judged whether the application which serves as a host needs an user validation for installation of this plug-in with reference to the security policy in security policy DB201b while receiving the above-mentioned list in that security management department 201a (Step S702). if it confirms whether the function specified beforehand is included and is specifically contained during the shown list -- a check important point -- if not contained -- a check -- suppose that it is unnecessary.

[0070]And if the user validation is required (Step S702: Yes), A dialog as shown in drawing 4 by the execution propriety inquiry part 201d is displayed (Step S703), and when the "yes" button 400 is pushed in the dialog of the figure, (Step S704:Yes) and a dialog as further shown in drawing 5 are displayed (Step S705). Then, it carries out usually through installation of the plug-in concerned (Step S706), and processing by this flow chart is ended.

[0071]Instead of performing (Step S704:No) and installation, when the "no" button 401 is pushed in the dialog of drawing 4, the message of the purport that installation was stopped is displayed (Step S707), and processing by this flow chart is ended.

[0072]The procedure of the prevention from program execution by motive stop shown in drawing 8 below is explained. If plug-in is called from the application which serves as the host, the functional listing presentation part 200a will show the list of functions which is planning use (Step S801). In a host, it is judged by that security management department 201a whether an user validation is required in advance of starting of this plug-in (Step S802).

[0073]It is specifically a dialog (Step S705 of drawing 7) of drawing 5 at the time of installation. It is a case where it is set up also check again just before starting, and when the function beforehand specified in the functional listing shown above is included, it judges with an user validation being required (Step S802: Yes). And it points in the execution propriety inquiry part 201d, and a dialog as shown in drawing 4 is displayed (Step S803).

[0074]If the "yes" button 400 is pushed in this dialog (Step S804: Yes), If it starts usually through plug-in (Step S805) and the "no" button 401 is pushed (Step S804: No), after displaying the message of the purport that starting of plug-in was stopped (Step S806),

processing by this flow chart is ended.

[0075]The procedure of the prevention from program execution by execution discontinuation shown in drawing 9 below is explained. The system-protection part 201e points that there is a call of a function from the function call part 200b of plug-in to the application which serves as the host in the security management department 201a (Step S901). It is made to judge whether the function concerned is what may be performed without an user validation (Step S902).

[0076]The security management department 201a is a function in which the function concerned was beforehand specified by the security policy set part 201c. And when it differs from the function shown before execution (just before installation and/or starting), it judges with a user's check being required (Step S902: Yes), and it points in the execution propriety inquiry part 201d, and a dialog as shown in drawing 6 is displayed (Step S903).

[0077] And perform processing called when "continuation" button 600 was pushed in this dialog (Step S904: Yes). Namely, execution of plug-in is continued as it is (Step S905). If the "stop" button 601 is pushed (Step S904: No, step S906:Yes), while interrupting execution of plug-in at the time, the fact will be displayed by a message (Step S907).

[0078]If "uninstallation" button 602 is pushed (Step S906: No), after uninstalling the plug-in concerned (Step S908), processing by this flow chart will be ended.

[0079]Although it waited for a user's directions and an installation stop, a starting stop, or execution discontinuation was performed in the embodiment mentioned above, Or when the function beforehand specified in the shown functional listing is included, or when the function which is not into the functional listing shown beforehand is called, it does not wait for a user's directions but may be made to perform a stop and discontinuation compulsorily.

[0080]Although checking to a user by the functional unit which a program uses set up whether would lend and there would be in the embodiment mentioned above (drawing 3), checking for every program may enable it to set up whether lends and there is. For example, when one PC is being used by two or more persons, so that dangerous plug-in (plug-in etc. which is not certain as for a source) may not be easily introduced by other users, The management representative specifies plug-in beforehand, and when the other plug-in becomes installed, it may be made to display warning like drawing 4.

[0081]The program which realizes each above-mentioned function part can be stored in various recording media, such as FD107 besides HD105, CD-ROM113, or MO, and can be distributed with the recording medium concerned. Distributing via a network is also

possible.

[0082]The security management department 201a shown in drawing 2 is equivalent to the "judging means", the "1st judging means", and the "2nd judging means" which are said to a claim, and the processing to perform is equivalent to the "determination process", the "1st determination process", and the "2nd determination process" which are said to a claim so that clearly also from the above-mentioned explanation.

[0083]The processing to perform is equivalent to the "setting means" which the security policy set part 201c says to a claim at the "specification process" said to a claim. The processing to perform is equivalent to the "inquiring means" which the execution propriety inquiry part 201d says to a claim at the "inquiry process" said to a claim.

[0084]As explained above, when the function in which there is a possibility of giving a damage to a user and a system is included in plug-in according to the embodiment of the invention, Since installation and starting of the plug-in concerned are refused according to a user's judgment, the damage which may be produced as a result of performing the plug-in concerned is beforehand avoidable.

[0085]Without trusting easily the functional listing shown before execution, since the credibility is continuously monitored also during execution, plug-in which it tries to call secretly while performing the dangerous function which has not been notified a priori can be stopped, just before the function concerned is called. The effect brought about by this is the same as that of the above.

[0086]And regardless of whether this invention is the program created with whether it is the program infected with the virus on the principle, and a certain bad faith, Since the execution can be prevented if operation dangerous for a user or a system is carried out, the usual program which was difficult for indication, and a program with the bad faith which distinction does not attach are also easily detectable by conventional technology.

[0087]Even if it is the pleiomorphia type virus which is increasing in recent years, as long as the processing made into the purpose is the same, it has the feature that it is detectable irrespective of the difference in an external code. And the work which does not need to prepare the virus definition file (it is called a pattern file, a DAT file, etc.) which covered the code group of all the viruses, and updates the file concerned frequently for the detection is also unnecessary.

[0088]Since this invention prevents execution of a program by very simple judgment [say / whether a thing dangerous in the function which is due to be called as mentioned above is contained or the actually called function was notified a priori], There is also a realistic merit that it is enforced strictly reasonable every day and effectiveness can be

planned without requiring a long time like the conventional virus scan.

[0089] Since the function which can be used like Java of conventional technology is not restricted uniformly, the flexibility of a program is able to aim at coexistence of increase, safety, and convenience.

[0090] Especially in the embodiment mentioned above, execution propriety was judged about plug-in in the application which serves as the host in the program, and it is also possible to apply this invention, for example to the relation between a broad view and the application concerned which carries out macro operation.

[0091] This invention is applied between general application and OS, namely, the function of discontinuation of the program under the stop of installation of a program, a motive stop, or execution can also be given to the OS itself. By this, it will be equivalent to introducing antivirus software etc. separately, or the safety effect beyond it will be acquired.

[0092] Drawing 10 is an explanatory view showing typically how execution of application is prevented, when OS is made to possess the program execution preventing function by this invention. The figure shows the example interrupted when the application once permitted installation and starting calls during execution the file deletion function which is not during the above-mentioned list by presentation of the functional listing of camouflage.

[0093]

[Effect of the Invention] As explained above, the invention according to claim 1, The judging means which judges whether the function specified by said setting means in the setting means to which a user's permission specifies a required function as the execution, and the functional listing shown from the program is included, Since it had the inquiring means which asks a user whether install said program when judged with said specified function being included by said judging means in said functional listing, About the program which performs processing specified beforehand. While being warned to a user of the fact in advance of installation, when a user points, it is stopped by the installation concerned and by this. The effect that the program execution arrester which can prevent execution of a program dangerous for a user or a system beforehand is obtained is done so.

[0094] The setting means to which the invention according to claim 2 specifies a function for a permission to be granted [of a user] as the execution, The judging means which judges whether the function specified by said setting means in the functional listing shown from the program is included, Since it had the inquiring means which asks a user whether start said program when judged with said specified function being

included by said judging means in said functional listing, About the program which performs processing specified beforehand. While being warned to a user of the fact in advance of starting, when a user points, the starting concerned is stopped and the effect that the program execution arrester which can prevent execution of a dangerous program beforehand for a user or a system by this is obtained is done so.

[0095]The setting means to which the invention according to claim 3 specifies a function for a permission to be granted [of a user] as the execution, The 1st judging means that judges whether the function called from the program is a function specified by said setting means, The 2nd judging means that judges whether it was contained in the functional listing shown said called function from said program when judged with said called function being said specified function by said 1st judging means, The inquiring means which asks a user whether continue execution of said program when judged with not having been contained in the functional listing shown said called function from said program by said 2nd judging means, When a function which is different from having been beforehand shown during execution of a program by that of ***** is called, While being warned to a user of the fact, when a user points, execution of the program concerned is interrupted, and the effect that the program execution arrester which can prevent execution of the problem portion of a dangerous program beforehand for a user or a system by this is obtained is done so.

[0096]The specification process to which the invention according to claim 4 specifies a function for a permission to be granted [of a user] as the execution, The determination process which judges whether the function specified at said specification process in the functional listing shown from the program is included, Since the inquiry process of asking a user whether install said program was included when judged with said specified function being included in said functional listing by said determination process, About the program which performs processing specified beforehand. While being warned to a user of the fact in advance of installation, when a user points, it is stopped by the installation concerned and by this. The effect that the program execution prevention method which can prevent execution of a program dangerous for a user or a system beforehand is acquired is done so.

[0097]The specification process to which the invention according to claim 5 specifies a function for a permission to be granted [of a user] as the execution, The determination process which judges whether the function specified at said specification process in the functional listing shown from the program is included, Since the inquiry process of asking a user whether start said program was included when judged with said specified function being included in said functional listing by said determination process, About

the program which performs processing specified beforehand. While being warned to a user of the fact in advance of starting, when a user points, the starting concerned is stopped and the effect that the program execution prevention method which can prevent execution of a dangerous program beforehand for a user or a system by this is acquired is done so.

[0098]The specification process to which the invention according to claim 6 specifies a function for a permission to be granted [of a user] as the execution, The 1st determination process that judges whether the function called from the program is a function specified at said specification process, The 2nd determination process that judges whether it was contained in the functional listing shown said called function from said program when judged with said called function being said specified function by said 1st determination process, The inquiry process of asking a user whether continue execution of said program when it judges that it was not contained by said called function in the functional listing shown from said program by said 2nd determination process, When a function which is different from having been beforehand shown during execution of a program by ***** is called, While being warned to a user of the fact, when a user points, execution of the program concerned is interrupted, and the effect that the program execution prevention method which can prevent execution of the problem portion of a dangerous program beforehand for a user or a system by this is acquired is done so.

[0099]Since the invention according to claim 7 makes a computer perform the method of any one statement of said claim 4 - claim 6, The method of any one statement of said claim 4 - claim 6 is read by computer, is performed, and by this. The effect that a user, a program dangerous for a system, or the program that can prevent execution of the problem portion beforehand at least is acquired is done so.

[0100]Since the invention according to claim 8 recorded said program according to claim 7, Said program according to claim 7 is read by computer, and is executed, and the effect that a user, a program dangerous for a system, or the recording medium that can prevent execution of the problem portion beforehand at least is obtained by this is done so.

DESCRIPTION OF DRAWINGS

[Brief Description of the Drawings]

[Drawing 1]It is an explanatory view showing the hardware constitutions of the program execution arrester concerning an embodiment of the invention.

[Drawing 2]It is an explanatory view showing functionally the composition of the program execution arrester concerning an embodiment of the invention.

[Drawing 3]It is an explanatory view showing an example of the screen for setting up the details of a security policy displayed by the security policy set part 201c.

[Drawing 4]It is an explanatory view showing an example of the dialog for checking the execution propriety before plug-in execution displayed by the execution propriety inquiry part 201d.

[Drawing 5]It is an explanatory view showing an example of the dialog for setting up whether execution propriety is checked also just before starting of plug-in displayed by the execution propriety inquiry part 201d.

[Drawing 6]It is an explanatory view showing an example of the dialog for checking the execution propriety during plug-in execution displayed by the execution propriety inquiry part 201d.

[Drawing 7]It is a flow chart which shows the procedure of the program execution preventing process by the stop of installation in the program execution prevention system concerning an embodiment of the invention.

[Drawing 8]It is a flow chart which shows the procedure of the program execution preventing process by starting stop in the program execution prevention system concerning an embodiment of the invention.

[Drawing 9]It is a flow chart which shows the procedure of the program execution preventing process by execution discontinuation in the program execution prevention system concerning an embodiment of the invention.

[Drawing 10]When this invention is applied to OS, it is an explanatory view showing typically how execution of application is prevented.

[Description of Notations]

100 A bus or a cable

101 CPU

102 ROM

103 RAM

104 HDD

105 HD

106 FDD

107 FD

108 Display

109 Network I/F

110 Telecommunication cable

111 Keyboard
112 Mouse
113 CD-ROM
114 CD-ROM drive
200a Functional listing presentation part
200b Function call part
201a Security management department
201b Security policy DB
201c Security policy set part
201 d Execution propriety inquiry part
201e System-protection part
201 f File reading part
201g file deletion part
201 h Window generation part
201i Text outputting part

*** NOTICES ***

JPO and INPIT are not responsible for any
damages caused by the use of this translation.

1.This document has been translated by computer. So the translation may not reflect
the original precisely.

2.*** shows the word which can not be translated.

3.In the drawings, any words are not translated.